IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. RUSLAN YELISEYEV, Defendant.	Case No. 16-CR-310 Hon. Claude M. Hilton Sentencing: Aug. 17, 2018

POSITION OF THE UNITED STATES ON SENTENCING

For over six years, the defendant, Ruslan Yeliseyev, trafficked in personal financial information that had been stolen from over **62,000 victims**. Born in Odessa, Ukraine, the defendant has been active on Russian-speaking cybercrime forums since at least 2001. Using the criminal contacts he gained through these forums, the defendant acted as a middle-man between large-scale computer hackers and retail-level fraudsters. He would obtain victims' payment card information, which had been obtained through computer hacking, and a sell it on exclusive, underground websites designed to facilitate the trafficking of stolen financial information and the resulting fraud. In addition, the defendant harvested victims' online banking credentials from so-called "botnets," or networks of infected computers, and provided that information to a co-conspirator in exchange for a share of the resulting fraud.

The presenetence report properly calculated the defendant's guidelines range as **97-121 months** in prison. The government respectfully submits that a sentence within this range is necessary to reflect the breadth of the harm caused, and to deter a new type of crime that continues to ensnare more and more Americans every single day.

I. Offense of Conviction

The defendant was arrested while visiting Israel on December 6, 2016, pursuant to a provisional arrest warrant. On December 22, 2016, he was indicted by a federal grand jury in this district for wire fraud, access device fraud, and conspiracy to commit wire fraud. PSR ¶ 1.[1] After fighting extradition from Israel for almost a year, the defendant agreed to waive extradition in November 2017 and was transported to the United States in January 2018.[2] On May 22, 2018, the defendant pled guilty to conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1343. In connection with that plea, the defendant admitted to trafficking in stolen financial information for over six years. PSR ¶ 10. Specifically, he admitted to trafficking in and possessing over 62,000 stolen payment card numbers, and to providing stolen online banking credentials to a co-conspirator, knowing that his co-conspirators would use the victims' stolen financial information to steal money from the victims' bank accounts and to make purchases on the victims' credit cards. PSR ¶¶ 16-19.

II. Guidelines Range

The probation officer correctly calculated the defendant's offense level as follows:

Guideline	Offense Level
Base Offense Level (Sections 2B1.1(a)(2))	7
Loss amount between $25 and $65 Million (Section 2B1.1(b)(1)(L))	+22
Substantial part of offense committed abroad (Section 2B1.1.(b)(10))	+2

[1] The PSR incorrectly states that the indictment was on December 22, 2017. The correct date is December 22, 2016.

[2] The defendant was detained in Israel from December 6, 2016 through January 11, 2018, pursuant to a provisional arrest request from the United States for charges connected with this case, and not based on any crime under Israeli law. Accordingly, the Bureau of Prisons should count that time towards the sentence the Court imposes in this case and will do so unless the Court orders to the contrary. *See* 18 U.S.C. § 3585(b)(1).

Offense involved the trafficking in any unauthorized access device (Section 2B1.1(b)(11))	+2
Acceptance of responsibility (Section 3E1.1)[3]	-3
TOTAL	**30**

PSR ¶¶ 29-40. Based on the defendant's Category I Criminal History, the resulting guidelines range is **97-121 months' imprisonment**. *Id.* ¶ 72.

III. Incarceration Recommendation

As the Court is well aware, the Sentencing Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[4] Here, however, a within-guidelines sentence is also supported by the other § 3553(a) factors, particularly the need for a sentence that reflects the seriousness of the offense and adequately deters others from perpetrating similar crimes.

A. The Sentence Should Reflect the Harm Caused to Individuals and to the Banking Industry and its Customers.

The full harm caused by the defendant's scheme is hard to calculate. The defendant admitted to trafficking in stolen credit and debit card information for at least six years. In one instance, the government was able to gain access to 213 stolen credit card numbers purchased by

[3] Provided that the defendant continues to accept responsibility, the Government intends to move at sentencing for a third point to be reduced from the defendant's offense level under U.S.S.G. § 3E1.1(b).

[4] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

the defendant and determine that they were ultimately used to make over $32,000 in unauthorized purchases and withdrawals. PSR ¶ 24. On two other instances, the government can show that the defendant advertised for sale on cybercrime forums 50,000 and 12,000 stolen credit card numbers. PSR ¶ 18. Because the government does not have access to the particular credit card numbers that the defendant advertised and presumably sold on cybercrime forums, it is not possible to calculate the actual fraud that resulted. It is precisely because of these types of difficulties in tying stolen access devices to particular frauds, however, that the U.S. Sentencing Commission has adopted a conclusive presumption that the loss associated with each stolen access device "shall be not less than $500." U.S.S.G. § 2B1.1, app. note 3(F)(i). Accordingly, the parties have stipulated that the loss associated with the over 62,000 stolen payment card numbers that the defendant trafficked in is over $31 million. PSR ¶ 30.

B. The Sentence Should Reflect the Defendant's Role in the Infrastructure that Supports Computer Hacking.

Just like drug dealers, computer hackers need distribution networks. Major computer intrusions often involve the stolen personal or financial information of hundreds, thousands, or even millions of victims—volumes that are far above what any one person could monetize. Hackers therefore need distribution networks to pass stolen financial information from the large-scale hacker all the way down to the street-level fraudster. For over 6-years, the defendant was a key player in that distribution network: he received bulk amounts of stolen financial information from co-conspirators in Russia and/or Eastern Europe and sold passed that information to co-conspirators, knowing that it would be used to steal money from the victims. The defendant

therefore played a critical role in an organized crime network that incentivized computer hacking and magnified its harms. He should be sentenced accordingly.

IV. Conclusion

The government respectfully recommends that the Court impose a sentence of 97-121 months' imprisonment, and enter agreed forfeiture and restitution orders of $207,366.20, and $32,283.50, respectively.

G. Zachary Terwilliger
United States Attorney

By: /s/
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov

August 10, 2018

Certificate of Service

I hereby certify that on this day, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on this day, I will send a true and correct copy of the foregoing by e-mail to the following:

Jennifer D. Lyerly
United States Probation Officer
jennifer_lyerly@vaep.uscourts.gov

By: /s/
Kellen S. Dwyer
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov